AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of California

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Google, Inc.
1600 Amphitheater Parkway, Mountain View, CA

Case No. '13 MJ8494

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

see Attachment A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

see Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 2320; 18 USC 1956; 18 USC 1341; 18 USC 1343; 26 USC 7201; 26 USC 7206	Trafficking of counterfeit goods and services; money laundering; mail fraud; wire fraud; tax evasion; and filing of false tax returns

The application is based on these facts:

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Christiansen Madsen, Special Agent ICE/HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: 6-19-2013 @ 9:35a.m.

Judge's signature

City and state: EL CENTRO, CALIFORNIA

HON. PETER C. LEWIS, U. S. MAGISTRATE JUDGE
Printed name and title

(1) kcm

ATTACHMENT A

Place to Be Searched

Google, Inc. is an Internet Service Provider with its primary computer information systems and other electronic communications and storage systems, records and data located at 1600 Amphitheater Parkway, Mountain View, California 94043.

ATTACHMENT B

I. Service of Warrant

The officer executing the warrant shall permit Google, Inc. (the "ISP"), as custodian of the files described in Section II, to locate and copy them onto removable electronic storage media and deliver the same to the officer.

II. Data to Be Supplied by the ISP

The ISP shall copy to electronic storage media all files [including emails, attachments, buddy lists, profiles, access logs, transactional data, billing records, and any other related financial, subscriber, and user records] associated with **sumaliba@gmail.com** ("the subject account") for the period January 1, 2012 to the date this warrant is signed.

III. Search and Seizure of Data by Law Enforcement

Law enforcement shall conduct any search of the data pursuant to the "Procedures For Electronically Stored Information" section of the affidavit supporting the search warrant. Law enforcement is authorized to seize data **limited to:**

A. The purchase, sale, or shipment of counterfeit cellular phone parts or other counterfeit electronics;

B. The resale of counterfeit cellular phone parts or other counterfeit electronics in the United States;

C. The receipt or distribution of payments for counterfeit cellular phone parts or other counterfeit electronics; and

D. The dominion and control of the subject account,

evidencing (1) trafficking in counterfeit goods in violation of 18 U.S.C. § 2320, (2) money laundering in violation of 18 U.S.C. § 1956, (3) mail fraud in violation of 18 U.S.C. § 1341, (4) wire fraud in violation of 18 U.S.C. § 1343, (5) tax evasion in violation of 26 U.S.C. § 7201, or (6) filing false returns in violation of 26 U.S.C. § 7206(1).

AFFIDAVIT

I, Christiansen C. Madsen, being duly sworn, state as follows:

I. INTRODUCTION

A. Training and Experience

1. I am a Special Agent with the U.S. Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations with the Department of Homeland Security. I have been so employed since January 3, 2010. Prior to my employment with ICE, I served as a United States Secret Service Uniformed Division Officer from October 2004 to January 2010.

2. I am a graduate of the Federal Law Enforcement Training Center ("FLETC"). At FLETC, I received training in criminal investigative techniques, including financial investigations, the execution of search warrants, and other areas of law enforcement. Since becoming an agent, I have also received both formal and on-the-job training in the laws and regulations relating to the trafficking of counterfeit goods and services, money laundering, mail fraud, and wire fraud. I have also directed, and participated in, numerous investigations that involved these crimes. Additionally, I have led and/or participated in dozens of search warrants, including several electronic search warrants that targeted commercial fraud. I also communicate regularly with investigators with expertise in computers, computer forensics, and internet-based investigations. As a federal agent, I am authorized to investigate violations of laws of the United States and I

am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

B. Purpose of This Affidavit

3. This affidavit is made in support of an application for a search warrant for the below-listed Internet Service Provider ("ISP") and respective email account:

a. Google, Inc. ("Google"), 1600 Amphitheater Way, Mountain View, California 94043 (described in Attachment A) for the following email account:

sumaliba@gmail.com (described in Attachment B).

4. The statements in this affidavit are based on my training and experience, my personal knowledge, my participation in other federal investigations, my conversations with other law enforcement agents and third parties, and my review of records obtained during this investigation. Because this affidavit is submitted for the limited purpose of securing the search warrant as described herein, it does not include every fact known to me concerning the investigation. I set forth only the facts necessary to establish that probable cause exists to believe that evidence of trafficking of counterfeit goods and services (18 U.S.C. § 2320), money laundering (18 U.S.C. § 1956), mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), tax evasion (26 U.S.C. § 7201), and filing of false returns (26 U.S.C. § 7206(1)) (more particularly described in Attachment B) will be located within the servers and records of the ISP listed above (more particularly

described in Attachment A). It is my opinion that such probable cause exists based on the information set forth below.

II. PROBABLE CAUSE

A. Background

5. In March 2012, Apple, Inc. ("Apple") notified law enforcement that the website flexqueen.com was possibly trafficking in counterfeit goods. Based on a variety of investigative measures that include seizures of counterfeit goods from Flexqueen, agents have determined that Flexqueen sells counterfeit cellular phone parts and other electronics to customers in the United States and abroad primarily through its website. Sales records indicate that Flexqueen purchases the counterfeit goods from a Chinese supplier. Payment records indicate Flexqueen averages well over $1,000,000 in online sales alone. Thus far, agents have not identified any authentic items sold by Flexqueen.

6. Based on records related to purchases of counterfeit items from flexqueen.com by an undercover agent and investigators from Apple, agents have determined that Flexqueen and Ocesa Manufacturing are the same entity. For example, Apple received a bill from "Flexqueen/Ocesa Manufacturing" after it purchased a counterfeit Apple part through the flexqueen.com website. The same email revealed that Ocesa Manufacturing operates a second website, ocesa.com, which also sells cellular phone parts and other electronics-related items.

7. In November 2012, agents executed a court-authorized search warrant of flexqueen.com and its attendant email accounts (hereinafter "November 2012 search"). Records received indicate, among other things, that: (1) the website was started on September 7, 2007; (2) it is registered to Yolanda Martinez, with Ricardo Puente as the listed registrant for the PayPal account linked to Flexqueen.com for payment processing; (3) Puente runs a Flexqueen-affiliated store in Mexico; (4) the accounts duhongwei88@hotmail.com and the subject account, **sumaliba@gmail.com**, are used by an individual (believed to be a Chinese national named Hongwei Du, aka "Nick Du") who supplies Flexqueen with counterfeit goods; and (5) amcellular@hotmail.com is an email account used by the self-described owner of Flexqueen, Octavio Sana ("Sana"), and other Flexqueen personnel.

8. A records check for ocesa.com revealed that its website administrator is "Abel Sana." Law enforcement database checks show that Abel Sana is associated with 1248 E. Calle De Oro, Calexico, California. California Department of Motor Vehicles ("DMV") records list this address as the residence for Octavio Sana. Sana was the listed consignee (i.e., ultimate recipient) on numerous importations of electronics from China from January 2012 through February 2013 that were shipped to Flexqueen/Ocesa Manufacturing at 1356 Truman Court, Calexico, California and his storefront located at 656 9th Avenue, San Diego, California. Surveillance has identified 1356 Truman Court, Calexico, California as Flexqueen's main address, although employees have referenced

other locations like the store operated by Puente, in emails. Agents have seen stacked boxes that nearly fill the entire two-car garage of the Truman residence and have observed individuals make what appear to be daily mail runs to local post offices. And, in a letter attached to an email found pursuant to the November 2012 search, Sana identified himself as the owner of flexqueen.com. The letter, dated November 28, 2012, appears to have been a reference for Petra Ramirez Yolanda Lerma (aka "Yolanda Martinez"), a Flexqueen employee and coconspirator who, based on Sana's letter, works at Flexqueen's "Mexicali, BC, Mexico" office.

9. Emails indicate that Saduan Electronic, Du's company, is Flexqueen's primary – and possibly sole – source for counterfeit goods. United States Customs' records, however, show that Flexqueen and Sana received cell phone parts and other electronics from approximately 50 Chinese exporters from January 2012 to February 2013, including Saduan. Emails indicate that in addition to directly shipping counterfeit goods to Flexqueen, Saduan utilizes these third-party exporters as well. A review of law enforcement databases revealed that United States law enforcement has seized a variety of counterfeit goods (e.g., electronics, dvds, personal care items, tax-exempt cigarettes) shipped by approximately 28 of the companies that have exported electronics from China to Flexqueen.

10. Agents have also conducted multiple undercover purchases of several products that were subsequently confirmed as counterfeit items. In May 2012, agents

purchased a number of items from flexqueen.com that purported to be Apple iPhone parts (they were all marked with either the Apple logo or the word "APPLE"). After the purchases, Apple determined that the purchased items were counterfeit. And on June 1, 2012, an undercover agent ("UC-1") contacted Flexqueen and posed as a potential buyer of large quantities of counterfeit cell phone parts. Agents recorded conversations UC-1 had with a former Flexqueen employee, Angela Vela.[1] During the conversations, Vela acknowledged that Flexqueen sold counterfeit parts. For example, in response to UC-1 statement that Flexqueen sold high quality counterfeit parts, Vela responded, "Yeah." And when UC-1 told Vela that one of Flexqueen's products looked "exactly like it came from Apple," Vela responded, "Right." Vela later told UC-1 that Flexqueen had iPhone 4S kits (the external covers for the iPhone 4S phone) "in all different types of colors." Vela continued, "No, I don't think they [Apple] have this many, or this variety of colors." Apple confirmed that legitimate iPhone 4S kits only come in white or black. Vela also quoted UC-1 prices for different items and offered that if they did the deal in person, UC-1 "can, like, not worry about tax and shipping and all that." UC-1 eventually agreed to buy 250 iPhone digitizer screens. When they met to complete the deal, Vela explained, "The only thing that will get you in trouble on that is the actual Apple logo on the back." Vela told UC-1 that the shipment should be available the following week, as it was arriving from "Asia."

[1] Vela told UC-1 on June 7, 2013 that she was fired from Flexqueen because Sana was not happy with the day-to-day operation of the business and wanted to take a more active role.

11. On July 10, 2012, agents identified the suspected shipment that Vela referenced at the Los Angeles International Airport. The shipment was from Saduan Electronic (Du's company) and intended for the "Imperial Valley Trading Company" at Flexqueen's Truman Court address in Calexico. Agents seized approximately 600 electronics parts, including 345 LCD digitizer screens that purported to be manufactured by Apple (the word "APPLE" was stamped on a cable attached to the screens) pursuant to a search of the Saduan shipment. Apple confirmed that the digitizer screens were counterfeit. A Customs and Border Protection ("CBP") importations expert estimated the retail value of the items, if legitimate, to be approximately $187,498.

12. Following the seizure, on July 12, 2012, Vela emailed Sana at his amcellular@hotmail.com address: "DHL Package [sic] that is being held, is still being held, no additional information is needed. They will email me with more additional information tomorrow. I have already contacted [Undercover Agent's alias] concerning this, but no answer back from him yet."

13. As noted above, Flexqueen operates multiple locations in addition to its Calexico address. Email records indicate they maintain at least one location in Mexico and agents have observed Sana operating a store front in downtown San Diego called SD Cell Repair. For example, on September 11, 2012, a plain-clothes agent inquired with Sana at SD Cell Repair about the cost to repair a screen for a Samsung Epic Galaxy cell phone. The agent observed Sana look up the item's price on flexqueen.com. The agent

then asked Sana about iPhone LCD screens and back covers, which were marked with the Apple logo, in an assortment of colors such as pink, green, purple, and red. When the agent asked Sana how he had "iPhone" covers in these colors when Apple only makes them in black and white, Sana replied that the covers were "generic, not original." Sana also told the agent he had a replacement battery for a Samsung Epic cell phone available for $10 because it too was "generic," not original. Sana showed the agent a replacement battery and remarked that it looked exactly like an original battery. The agent purchased the battery for $10. Sana did not provide the agent with a receipt. Inspection of the battery revealed the word "Samsung" printed on the exterior of the battery. Samsung later confirmed that the battery purchased by the agent on September 11, 2012 from Sana's SD Cell Repair location was counterfeit.

B. Du and Other Target Subjects Use the Subject Account In Furtherance of Their Scheme to Sell Counterfeit Goods

14. Agents know from a review of Flexqueen email accounts that Flexqueen personnel communicate with Du over his **sumaliba@gmail.com** email address. For instance, based on agents' review of Flexqueen email accounts obtained pursuant to the November 2012 search, from June 26, 2012 to November 7, 2012, Du used the **sumaliba@gmail.com** email address approximately 10 times to communicate with Flexqueen email addresses. For instance, in an August 16, 2012 email about the July 10 seizure, Du explained to Vela that only the "branded" items, meaning those items with

identifiable, counterfeited, trademarks were seized. Du further told Vela that Flexqueen should have received the remainder of the "unbranded" shipment, meaning those items with no identifiable trademarks. In fact, CBP seized the items with trademarks on them but allowed those items with no commercial markings to be delivered.

15. Flexqueen personnel have also used **sumaliba@gmail.com** to place orders for counterfeit items with Du. For example, on November 6, 2012, Vela sent an order to Du's **sumaliba@gmail.com** account for several products Flexqueen needed, including some parts that are obviously counterfeit (e.g., "iPhone 4 GSM Pink Kits") – again, Apple does not make such kits in any colors other than black or white.

16. The emails from Vela to Du's **sumaliba@gmail.com** also substantiated agents' belief that Sana maintains a leadership role with Flexqueen. While Vela provided Du with a general list of items Flexqueen needed, she instructed Du to follow up with Sana about the specifics of Flexqueen's order. She wrote, "[P]lease confirm with Octavio first on things we need." Subsequent emails between Vela and Du indicated that Du was trying to reach Sana via the online video chat provider, Skype. Vela told Du that Sana "replies when he can." She promised that she would contact Sana to let him know that Du was attempting to reach him.

17. Flexqueen email records also reflect that Du uses his **sumaliba@gmail.com** account to communicate directly with Sana. For example, on July 19, 2012, Du emailed Vela and Sana (amcellular@hotmail.com) to inform them that he had recently received

new "BB 9800 Dig," meaning Blackberry 9800 digitizers. Du also informed Sana and Vela that they received "3 unit defectives [sic] and 1 missing!!" Du appears to have been telling Vela and Sana that three units he received had defective parts and that he did not receive one unit that he had ordered. Du's reference to having received defective parts indicates two things: (1) the parts he is referring to are counterfeit; and (2) Saduan may not be the ultimate manufacturer of the counterfeit goods.

18. Finally, the November 2012 search revealed that Du uses the subject account to send Sana invoices of their transactions. For instance, on August 15, 2012, Du used **sumaliba@gmail.com** to email Vela and Sana (amcellular@hotmail.com) the "commercial invoice" for a recent shipment that he said was "for ur [sic] check." Emails and Customs records suggest that Du provides Flexqueen with two sets of invoices – one that accompanies the actual package through Customs inspection and a second that he sends to them directly via email. In my training and experience, I know that international counterfeiters will use "double invoicing" as a means of avoiding the full duties owed to Customs on imported items. The invoice that accompanies the shipment reflects a drastically reduced value of goods versus what the goods are actually worth. The distributor will then provide the buyer with a second invoice, in an email like this, which reflects the actual terms of the deal.

C. Du Uses of a Second Email Account to Communicate with Cell Phone Parts Suppliers

19. On May 2, 2013, the Court authorized a search of a second email account used by Du, duhongwei88@hotmail.com. The search revealed dozens of emails in which Du corresponds with cell phone parts suppliers about the sale and distribution of fraudulent cell phone parts and other electronics using the duhongwei88@hotmail.com account. For example:

a. On May 13, 2013, Du received an email from a parts manufacturer with a Chinese address. The parts manufacturer introduced himself and told Du that he specialized in supplying cell phone parts for several brand name phones, including Apple products. Agents believe the parts manufactured by this individual are counterfeit because, according to Apple, he is not an authorized Apple manufacturer. The agents' belief is further corroborated by the fact that the manufacturer refers to the parts as "after market, high quality" in his email.

b. On May 28, 2013, Du received an email from another Chinese manufacturer of cell phone batteries. The email had five Excel spreadsheets attached to it, which listed prices for brand name cell phone batteries the manufacturer had available. The lists of batteries were broken down by quality; for instance, one column of batteries was rated as "AAA+," while a second category of batteries was rated as "B-Grade." Agents believe the batteries offered were fraudulent, in part, because the lists contained the same batteries (e.g., Blackberry FS1 9800) as both "AAA+" and "B-Grade." The

AAA+ Blackberry FS1 9800 cost $4.15, while the "B-Grade" Blackberry FS1 9800 cost $2.82.

D. Target Subjects' Retention of Emails

20. Based on my training and experience, I know that individuals who utilize emails in furtherance of their criminal activities tend to retain the emails in their accounts for a long period of time. This is particularly true of individuals involved in commercial fraud, like here. As explained above, Flexqueen and Saduan rely on their email communications to buy and sell counterfeit electronics parts. Previous email searches revealed several invoices sent and received over relevant Flexqueen and Saduan email accounts as well. Because of how they use email, it is common for them to retain the emails of their commercial transactions for a long period of time in order to maintain a record of any given transaction. In fact, the November 2012 search revealed emails that were almost four years old. Moreover, the emails obtained to date indicate that Flexqueen and Saduan personnel have little fear of their email traffic being discovered by law enforcement (thus, little cause for them to delete such communications). For instance, after the July 10, 2012 seizure of 600 counterfeit cell phone parts, not only did Du communicate with Flexqueen over the subject account, **sumaliba@gmail.com**, account about the seizure, but also about other orders as well. And the same was true for Vela's use of the admin@flexqueen.com account. Thus, not only is email critical to their

fraudulent scheme, but they are, apparently, operating with little fear of law enforcement detection of their email. These factors, along with my training and experience, cause me to believe that Du will retain relevant emails in the subject account at least as far back as January 1, 2012.

III. THE INTERNET SERVICE PROVIDER

21. Google, Inc. ("the ISP") is an ISP that, among other things, provides electronic communication services to subscribers. The ISP's electronic mail services allow subscribers to communicate with other subscribers and with others through the Internet. The ISP's subscribers access services through the Internet.

22. The ISP's subscribers use screen names during communications with others. The screen names may or may not identify the real name of the person using a particular screen name.

23. At the creation of an account with the ISP and for each subsequent access to the account, the ISP typically logs the Internet Protocol (IP) address of the computer accessing the account. An IP address is a unique address through which a computer connects to the Internet. IP addresses are leased to businesses and individuals by ISPs. Obtaining the IP addresses that have accessed a particular ISP account often identifies the ISP that owns and has leased that address to its customer. Subscriber information for that customer then can be obtained using appropriate legal process.

IV. PROCEDURES FOR ELECTRONICALLY STORED INFORMATION

24. Federal agents and investigative support personnel are trained and experienced in identifying communications relevant to the crimes under investigation. The ISP's personnel are not. It would be inappropriate and impractical for federal agents to search the vast computer network of the ISP for the relevant accounts and then to analyze the contents of those accounts on the ISP's premises. The impact on the ISP's business would be severe.

25. Therefore, I request authority to seize all content, including electronic mail and attachments, stored instant messages, stored voice messages, photographs and any other content from the ISP's account, as described in Attachment B. In order to accomplish the objectives of the search warrants with a minimum of interference with the business activities of the ISP, to protect the rights of the subject(s) of the investigation and to effectively pursue this investigation, authority is sought to allow the ISP to make a digital copy of the entire contents of the account subject to seizure. The copy will be provided to me or to any authorized federal agent. The copy will be forensically imaged and the image will then be analyzed to identify communications and other data subject to seizure pursuant to Attachment B. Relevant data will be copied to separate media. The original media will be sealed and maintained to establish authenticity, if necessary.

26. Analyzing the data to be provided by the ISP may require special technical skills, equipment and software. It also can be very time-consuming. Searching by

keywords, for example, often yields thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrants. Merely finding a relevant hit does not end the review process. Certain file formats do not lend themselves to keyword searches. Keywords search text. Many common electronic mail, database and spreadsheet applications, which files may have been attached to electronic mail, do not store data as searchable text. The data is saved in a proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases dramatically.

27. Based on the foregoing, searching the recovered data for the information subject to seizure pursuant to these warrants may require a range of data analysis techniques and may take weeks or even months. Keywords need to be modified continuously based upon the results obtained. The personnel conducting the examination will complete the analysis within ninety (90) days of receipt of the data from the service provider, absent further application to this court.

28. Based upon my experience and training, and the experience and training of other agents with whom I have communicated, it is necessary to review and seize all electronic mails that identify any users of the subject account and any electronic mails sent or received in temporal proximity to incriminating electronic mails that provide context to the incriminating mails.

29. All forensic analysis of the imaged data will employ search protocols directed exclusively to the identification and extraction of data within the scope of this warrant.

V. REQUEST FOR SEALING AND PRECLUSION OF NOTICE

30. This is an ongoing investigation of which the target(s) is unaware. It is very likely, based upon the above, that evidence of the crimes under investigation exists on the ISP's server space subject to the control of the target. There is reason to believe, based on the above, that premature disclosure of the existence of the warrant will result in destruction or tampering with that evidence and seriously jeopardize the success of the investigation. Accordingly, it is requested that the warrant and all related materials be sealed until further order of the Court. In addition, pursuant to Title 18, United States Code, Section 2705(b), it is requested that this Court order the ISP to whom this warrant is directed not to notify anyone of the existence of the warrant, other than its personnel essential to compliance with the execution of the warrant until further order of the Court.

VI. CONCLUSION

31. Based on the foregoing, I believe probable cause exists to believe that the items in Attachment B constitute evidence of violations of 18 U.S.C. § 2320 (trafficking of counterfeit goods and services), 18 U.S.C. § 1956 (money laundering), 18 U.S.C. §

1341 (mail fraud), 18 U.S.C. §1343 (wire fraud), 26 U.S.C. § 7201 (tax evasion) and 26 U.S.C. § 7206(1) (filing of false returns), and that such items will be found at the location to be searched as described in Attachment A.

Christiansen Madsen, Special Agent
Homeland Security Investigations

Subscribed to and sworn before me on this 19th day of June, 2013.

HONORABLE PETER C. LEWIS
United States Magistrate Judge